IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

Randall S. SPRINGFIELD, et al. Confirmation No: 1231

Serial No: 09/824,595 Group Art Unit: 2135

Filed: April 2, 2001 Examiner: Gyorfi, T.

For: METHOD AND SYSTEM FOR PROVIDING A TRUSTED
FLASH BOOT SOURCE

REPLY BRIEF

Janyce R. Mitchell
Attorney for Appellants
Lenovo
Sawyer Law Group LLP

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

Randall S. SPRINGFIELD, et al.	Confirmation No: 1231
Serial No: 09/824,595	Group Art Unit: 2135
Filed: April 2, 2001	Examiner: Gyorfi, T.

For: METHOD AND SYSTEM FOR PROVIDING A TRUSTED FLASH BOOT SOURCE

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Sir:

Appellant herein files a Reply Brief to the Examiner's Answer, drafted in accordance with the provisions of 37 C.F.R. § 1.193(b)(1) as follows:

I. REAL PARTY IN INTEREST

A statement identifying the Real Party in Interest is contained in the Appeal Brief.

II. RELATED APPEALS AND INTERFERENCES

A statement identifying the related appeals and interferences is contained in the Appeal Brief.

III. STATUS OF CLAIMS

A statement identifying the status of the claims is contained in the Appeal Brief.

IV. STATUS OF AMENDMENT

A statement identifying the status of amendments is contained in the Appeal Brief.

V. SUMMARY OF THE INVENTION

The present invention provides method and system for evaluating a boot source in a computer system having a processor. The method and system comprise determining the boot source used by the processor each time the computer system boots. Thus, the source of the code used in booting the processor is determined. The determination of the boot source may include writing the identity of the boot source rather than the code actually executed, preferably in a first register. Specification, page 7, lines 1-2 (paragraph 18). For example, the location of a particular number of instructions may be written. Specification, page 6, lines 1-10 (paragraph 18). The method and system also include allowing the known boot source to be specified. The known boot source is preferably specified by writing the identity of the known boot source in a second register. Specification, page 7, lines 3-6 (paragraph 18). As a result, the boot source for the computer is determined (through the identity written) and can be verified using the known boot source. Specification, page 7, lines 6-9. Thus, the boot source can be checked to ensure that a trusted source (the known boot source) has been used. Consequently, a trusted boot source can be provided. Specification, page 7, lines 9-10.

For example, Figure 4 depicts one embodiment of a method 250 for providing a trusted boot source. Specification, page 7, lines 11-12. The known boot source is specified by writing the identity of the known boot source to a write-once register such as the second register 154, via step 252. Specification, page 7, lines 15-16. Each time the computer system boots, the identity of the boot source used is written to the first register 152, via step 254. Specification, page 7, lines 21-23. This identity may be the "identity of the source of the first one hundred instructions executed by the computer system 100 . . ." Specification, page 7, lines 21-22. The identity of the boot source written in step 254 is checked against the known boot source in step 256. Specification, page 8, lines 2-5. Thus, it can be determined whether the boot source used was the known boot source. The computer system may then take appropriate action, via step 258. Specification, page 8, lines 6-10. The appropriate action may include acts such as shutting down if the boot source and known boot source do not match.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) whether claims 1-12 are each unpatentable under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,678,833 (Grawrock) in view of U.S. Patent no. 6,161,177 (Anderson).

VII. ARGUMENTS

A. Summary of the Applied Rejections

A summary of the Applied Rejections is contained in the Appeal Brief. In a Final Office Action dated March 27, 2006, the Examiner rejected claims 1-14 under 35 U.S.C. § 103 as being unpatentable over Grawrock in view of Anderson. In response to Appellant's arguments in the Examiner's Answer, the Examiner stated "Appellant argues that the boot block identifier disclosed in the cited portion of Grawrock is not the recited identity . . . of the boot source. Examiner concedes that . . . Appellant's analysis is correct. However, . . . this is rectified by the Anderson reference." With respect to Anderson, the Examiner stated:

> While the BIOS identifying information is used to establish compatibility between the CPU and the chipset, Appellant has overlooked a more fundamental fact: in order to make the disclosed comparison, the system disclosed by Anderson must first select a BIOS for analysis out of a conventional EEPROM memory unit which

> is capable of storing a plurality of BIOS programs. . . Each BIOS, including the data that would otherwise identify the make and model of a particular CPU or chipset, area set of instructions residing at different addresses (i.e. locations) within said EPROM, and that consequently in order to obtain the information to make the comparison, the Anderson system must necessarily know what each BIOS's address is so as to be able to find it within said EEPROM.

With respect to Appellant's argument that Anderson does not teach or suggest writing the identity of the boot source each time the system boots, the Examiner disagreed, stating that "Anderson discloses that the current BIOS identifying information can be written as part of a crisis routine. . . It is conceivable that there could exist an instance of the Anderson invention that requires the crisis recovery routine each time the machine is booted. . . Furthermore, it is noted that the Examiner cited Grawrock to recite this limitation."

Appellant respectfully requests that the Board reverse the Examiner's final rejection of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 under 35 U.S.C. § 103 and the Examiner's final rejection of claims 7 and 14 under 35 U.S.C. § 103.

B. The Cited Prior Art

Grawrock describes a system which provides a boot block *identifier* from the boot block memory unit, either the first time the computer system starts up or each time the system starts up. Grawrock, col. 3, lines 57-67. In particular, Grawrock states that the:

> boot block memory unit loads and records its boot block identifier into the memory . . . Next, the boot block memory unit locates and loads the BIOS for execution . . . The BIOS (or a representation thereof) is loaded to the TPM and a BIOS identifier is recorded . . .

Grawrock, col. 4, lines 25-30. Thus, Grawrock does state that a BIOS identifier and the boot block identifier are recorded. However, the boot block identifier is a hash of "boot information." Grawrock, col. 3, lines 57-61. Grawrock further states that the "boot information" is basically an image or series of sub-images that collectively *represent* the boot block code. Grawrock, col. 3, lines 45-50. Thus, the boot information corresponds to the boot code itself, rather than to an identity of the boot source. In response to challenges, a digital signature is provided. Grawrock, col. 4, lines 10-16. This digital signature is a combination of the boot block identifier, keying material, certificates, and other similar information. Grawrock, col. 4, lines 17-18. Consequently, Grawrock describes providing a boot block identifier and a digital signature incorporating the boot block identifier that are both based on a representation of the boot block code actually used rather than on the identity of the boot source.

Anderson is concerned with ensuring that the central processing unit (CPU) and BIOS are compatible. Anderson, Abstract. Thus, upon startup, the computer system executes a startup routine and BIOS located in a particular, apparently preset memory location. Anderson, col. 4, lines 32-43. Anderson also states that the system reads "identifying data" for the BIOS. Anderson, col. 4, lines 50-54. Anderson states that this "BIOS identifying data [is data] specifying the CPU or other chip set components corresponding to the BIOS program, i.e., the CPU that the BIOS program was designed to be executed by or the chip set components that the BIOS program was designed to operate with." Anderson, col. 3, lines 5-10. This identifying data is sufficient to determine whether the BIOS and hardware correspond to the same central processing unit and chip set. Anderson, col. 2, line 65-col. 3, line 20. Consequently, the identifying data apparently does **not** include the location of the BIOS. Anderson also states that the BIOS identifying data corresponds to the last executed BIOS program and is compared with stored hardware data. Anderson, col. 3, lines 22-26. Thus, it can be verified whether the BIOS program executed corresponds to the hardware. Anderson, col. 3, lines 27-35.

Anderson also describes performing a test upon each power up. Anderson, col. 4, line 50-col. 5, line 5. To do so, the system reads the hardware identifying data and data that relates to the BIOS. Anderson, col. 4, lines 50-54. As indicated above, the identifying data is apparently the CPU or other chip set components corresponding to the BIOS program. The information that has been read to determine whether the BIOS and hardware match. Anderson, col. 4, lines 54-60. If the information matches, no further action is taken. Anderson, col. 4, lines 60-61. If, however, the information does not indicate that the hardware and BIOS are compatible, then remedial action may be taken. Anderson, col. 4, lines 61-62. For example, selection of another BIOS or crisis recovery may be performed. Anderson, col. 3, lines 12-18. The crisis recovery in Anderson includes the user inserting a disk including the BIOS, and writing the BIOS to the appropriate memory locations. Anderson, col. 3, lines 18-26.

C. Claims 1-12 Are Not Unpatentable Under 35 U.S.C. § 103.

Appellant respectfully submits that the applied rejections of claims 1 and 6 under 35 U.S.C. § 103 are without merit as the Examiner has completely failed to explain why Grawrock in view of Anderson teaches or suggests the method and system recited in claims 1 and 6. Independent claims 1 and 6 recite a method and system, respectively, for evaluating a boot source in a computer system. In particular, method recited in claim 1 includes:

> determining the boot source used by the processor each time the computer system boots, the boot source determining further including writing an identity of the boot source, the identity of the boot source including a location of a particular number of instructions initially executed; and
>
> allowing the boot source to be specified once as a known boot source.

Similarly, independent claim 6 recites a system including:

> a first register for storing an identity of the boot source used by the processor each time the computer system boots, the identity of the boot source including a location of a particular number of instructions initially executed; and
>
> a second register for allowing the boot source to be specified once as a known boot source.

Thus, claims 1 and 6 recite that *each time the computer system boots*, the identity of the boot source is determined. This identity of the boot source includes the location of a number of instructions initially executed. Thus, each time the computer system boots, the identity of the boot source (including the location of instructions initially executed) is written. Consequently, it can be determined whether the boot source is a trusted boot source. Thus, the source, or location, of the instructions that are actually executed can be provided and independently verified. Specification, page 8, lines 13-15. Because the source of the instructions is verified, the boot source is evaluated and, therefore, trusted. As a result, a trusted boot source can be reliably provided. Specification, page 8, lines 15-16.

Grawrock in view of Anderson fails to teach or suggest writing an identity of the boot source, including writing the location of a number of instructions initially executed each time that the system boots. Appellant respectfully draws the Board's attention to the arguments made with respect to Grawrock and Anderson in the Appeal Brief. Further, nothing in the Examiner's Answer changes this conclusion. Grawrock discloses storing a "boot block identifier" for the boot source each time the system boots. As the Examiner has conceded, the boot block identifier of Grawrock is not the recited identify of the boot source (location of instructions initially executed). Consequently, the Examiner relies upon the "fundamental fact" of Anderson that a BIOS must be selected.

However, nothing in Anderson indicates that each time the computer system boots the identity of the boot source (locations of a number of instructions initially executed) is written.

First, selection of a BIOS does not imply that each time the computer system boots, the identity of the boot source (including the location of instructions initially executed) is written. Instead, Anderson merely indicates that the memory includes the BIOS as well as its identifying data. Anderson, col. 3, lines 3-10 and col. 4, lines 32-43. Thus, Anderson apparently reads BIOS located at specific, pre-selected memory locations. Thus, although Anderson selects the BIOS each time the system boots, this selection includes reading the BIOS stored at pre-selected memory locations. Consequently, Anderson's "selection" of a BIOS does not write the location of the BIOS each time the computer system boots.

Use of the identifying data in Anderson fails to teach or suggest writing the identity of the boot source each time the system boots. To determine whether the BIOS and hardware are compatible, the "identifying data" for the BIOS is obtained. This identifying data is the CPU or other chip set components corresponding to the BIOS, not the location of the BIOS itself. Consequently, any writing of the "identifying data" for the BIOS does not include writing the identity of the boot source each time the system boots.

The crisis recovery of Anderson also fails to teach or suggest writing the identity of the boot source each time the system boots. If a comparison of the BIOS identifying data and the hardware indicate that they don't match, then the system of Anderson takes other action. This action might include the crisis recovery cited by the Examiner. Crisis recovery in Anderson includes the user inserting a disk including the desired BIOS and writing the BIOS to the appropriate (again pre-selected) memory locations. Anderson, col. 3, lines 18-26. Anderson indicates that crisis recovery may only be performed if the hardware and BIOS are not compatible. Anderson, col. 3, lines 12-18. Consequently, the crisis recovery of Anderson is only performed if an error has been introduced. The Examiner's assertion that it is "conceivable" that an instance of Anderson requiring that crisis recover be performed "could exist" presumes that an error in the compatibility of the BIOS and hardware could exist each time the computer is booted. If so, the system of Anderson, particularly the crisis recovery of Anderson, would not function properly. Furthermore, if the crisis recovery is performed, then the BIOS is loaded from a user-inserted CD and the BIOS identifying information (i.e. compatible chip sets) stored. Anderson, col. 3, lines 18-26. Storing the BIOS and the identifying data is not the same as storing the *location* of instructions in the BIOS. Instead, the instructions themselves are written. Consequently, even if the crisis recovery were performed each time the system boots, the BIOS would be rewritten, not the BIOS' identity (location of a particular number of instructions initially executed). Various cited portions of Anderson, therefore, also fail to teach or suggest the method and system recited in claims 1 and 6.

If the teachings of Anderson were added to those of Grawrock, the combination would still fail to teach or suggest writing the identity of the boot source each time the system boots. As discussed above, both Grawrock and Anderson fail to teach or suggest writing the identity of the boot source each time the system boots. Consequently, any combination of Grawrock and Anderson would also fail to teach or suggest this feature. Stated differently, if Grawrock and Anderson were combined, then in addition to storing the boot block identifier of Grawrock, the combination might also perform the test of Anderson to determine whether the hardware and BIOS are compatible each time the system boots. However, none of writing the boot block identifier of Grawrock, using the BIOS identifying information, and crisis recovery include writing the location of a particular number of instructions initially executed. Consequently, Grawrock in view of Anderson fail to teach or suggest the method and system recited in claims 1 and 6, respectively. Accordingly, Appellant respectfully submits that claims 1 and 6 are allowable over the cited references.

Claims 2-5 and 7-12 depend upon independent claims 1 and 6, respectively. Consequently, claims 2-5 and 7-12 are allowable for the same reasons discussed above with respect to claims 1 and 6.

Accordingly Appellant respectfully requests that the Board reverse the final rejection of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 under 35 U.S.C. § 103.

D. Summary of Arguments

For all the foregoing reasons, it is respectfully submitted that Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 (all the claims presently in the application) are patentable for defining subject matter which would not have been obvious under 35 U.S.C. § 103. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Reply Brief, Appellant's "APPENDIX" section is contained on separate sheets following the signatory portion of this Reply Brief.

Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 50-3533 (Lenovo).

Very truly yours,

January 22, 2007

/Janyce R. Mitchell/Reg. No. 40,095
Janyce R. Mitchell
Attorney for Appellants
Reg. No. 40,095
(650) 493-4540

VIII. CLAIMS APPENDIX

1. A method for evaluating a boot source in a computer system having a processor comprising:

determining the boot source used by the processor each time the computer system boots, the boot source determining further including writing an identity of the boot source, the identity of the boot source including a location of a particular number of instructions initially executed; and

allowing the boot source to be specified once as a known boot source.

2. The method of claim 1 wherein the known boot source allowing step further includes:

specifying that the known boot source to be a FLASH boot source.

3. The method of claim 2 wherein the specifying step further includes:

writing the identity of the FLASH boot source in a write-once register which identifies the boot source for future boots.

4. The method of claim 1 wherein the determining step further includes:

writing the identity of the boot source in a register each time the computer system boots.

5. The method of claim 1 further comprising:

checking the boot source determined to ensure that the boot source is the known boot source.

6. A system for evaluating a boot source in a computer system having a processor coupled with a boot source, the system comprising:

a first register for storing an identity of the boot source used by the processor each time the computer system boots, the identity of the boot source including a location of a particular number of instructions initially executed; and

a second register for allowing the boot source to be specified once as a known boot source.

7. The system of claim 6 wherein the computer system includes a bridge coupling the processor with the boot source and wherein the first register and the second register are located in the bridge.

8. The system of claim 7 wherein the bridge is a south bridge.

9. The system of claim 6 wherein the known boot source is written only once to the second register.

10. The system of claim 9 wherein the known boot source is a FLASH boot source.

11. The system of claim 6 wherein the identity of the boot source is written to the first register each time the computer system boots.

12. The system of claim 6 wherein the processor is capable of checking the boot source stored in the first register to ensure that the boot source is the known boot source.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.